APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. PM 258042/SWS-89-US2/BB
(M#)

Invention: METHOD, SYSTEM AND GATEWAY ALLOWING SECURED END-TO-END ACCESS TO WAP SERVICES

Inventor (s): HUBER, Adriano
LOHER, Urs

Pillsbury Madison & Sutro LLP
Intellectual Property Group
1100 New York Avenue, NW
Ninth Floor
Washington, DC 20005-3918
Attorneys
Telephone: (202) 861-3000

This is a:

- ☐ Provisional Application
- ☒ Regular Utility Application
- ☐ Continuing Application
- ☐ PCT National Phase Application
- ☐ Design Application
- ☐ Reissue Application
- ☐ Plant Application
- ☐ Substitute Specification
  Sub. Spec Filed _____
  in App. No. _____/_____
- ☐ Marked up Specification re
  Sub. Spec. filed _____
  In App. No _____/_____

SPECIFICATION

Method, system and gateway allowing secured end-to-end access to WAP services.

This application claims priority of the provisional patent application US 60/152,356 and of the European patent application EP0810028.1, the contents of which are incorporated by reference.

TECHNICAL FIELD

The present invention concerns a method with which a mobile subscriber with a WAP-enabled terminal can access a WAP or WEB server.

BACKGROUND OF THE INVENTION

WAP (Wireless Application Protocol) servers, offering WAP-based services, are already known. Especially, WAP-based services in the field of e-commerce and of financial institutes are available.

Such services demand a secured transmission of the packets between the end-user and the server of the service provider. The usual solution recommended by the WAP forum makes use of the WTLS (Wireless Transport Layer Security) protocol layer; this method can, however, only be used to secure the packet transmission between the terminal and the gateway (possibly administered by a mobile network operator). In this gateway, a conversion of the protocol to the security protocol SSL 3.1 or to the TLS 1.0 is effected.

The principle of a data transmission secured by this method is shown schematically in figure 2. Reference number 1 shows a WAP-enabled terminal, for example a WAP-enabled GSM (Global System for Mobile Communication) mobile phone, that can connect over a digital mobile communication network 2 to a gateway administrated by the operator of this network. The terminal 1 contains a browser. Number 5 shows a server of a service provider, for example a financial institute or a provider in the field of e-commerce. This server can access a database 51 where WEB

and/or WAP pages are stored. The WEB or WAP pages can contain for example HTML, WML, JAVA-script, WML-script, etc. documents.

In order to access a WEB and/or WAP page in database 51, a user of terminal 1 has to send a request secured by WTLS services through the gateway 3 to server 5. This request is decrypted in gateway 3 through all the protocol layers of a converter module, then it is converted into a TLS or SSL-secured request that is sent over a TCP/IP network 4 to the server 5. In server 5, another converter module may be provided for converting this request into its own format that can be understood by the database administration system 51. The answer of server 5, for example the contents of a WEB and/or WAP page, is conveyed in the other direction through gateway 3, where it is converted, to the terminal 1.

This method does not allow for real end-to-end encryption; data and packets need to be decrypted and re-encrypted in gateway 3 to effect the protocol conversion. For many applications, such a security breach is however not acceptable.

One aim of the present invention is to propose a newer, more secure means of data transfer between a terminal and a WEB or WAP server.

Another aim is to propose a new method that allows end-to-end secured connection between a WAP-enabled terminal and a WEB or WAP server.

Another aim is to provide a new method that can be used with any WAP-enabled terminal using WTLS, specifically with terminals employing an authenticating of service based on a RSA key, on X.509v3 certificates, on RC5 or other security protocols according to WAP or WTLS or further digital certificates, respectively.

SUMMARY OF THE INVENTION

According to the present invention, these aims are achieved specifically with a method in which said terminal sends a request for said server to a WAP gateway, the security in the air interface between said WAP-enabled terminal and said gateway being based on WTLS (Wireless Transport Layer Security), said server containing a SSL and/or TLS protocol layer, the conversion between WTLS and SSL and/or TLS being effected in a secured domain administrated by the administrator of said server, and where the packets that are sent by said terminal are routed by said gateway to said secured domain without decrypting all the packets transmitted during a session.

The packets are transmitted through the gateway through a so-called tunnel layer without being decrypted. The contents thus remain confidential even for the operator of the gateway. The packets are then only decrypted at the server of the service provider in a proxy (a so-called E2ES-Proxy) and verified by a certificate of a trusted third party.

Furthermore these aims are achieved by a method with which a mobile subscriber with a WAP-enabled terminal can access a WEB or WAP server, said terminal sending a request for said server to a WAP gateway in which a browser in said terminal extracts the port number of the requested WEB or WAP pages and copies it into the packets sent to said gateway, and said packets in said gateway being routed depending on this port number.

Furthermore, these aims are achieved by securing the request that is sent by a terminal over a gateway to a WEB or WAP server with end-to-end WTLS.

Preferably, in the gateway one can differentiate between sessions that are to be handled conventionally and sessions to be routed according to the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Hereafter is a more detailed description of preferred embodiments of the invention with reference to the attached drawings, in which:

Figure 1 compares the protocol layers of a WAP protocol stack and of an internet protocol stack.

Figure 2 as described above shows the principle of secured data transmission according to the usual WAP protocol.

Figure 3 shows the principle of a secured data transmission according to a first embodiment of the invention.

Figure 4 shows the principle of a secured data transmission according to a second embodiment of the invention.

Figure 5 shows the principle of a secured data transmission according to a third embodiment of the invention.

DETAILED DESCRIPTION

Figure 3 shows the principle of a first embodiment of the invention. This figure shows a registered WAP-enabled terminal 1 in a digital mobile phone network, for example a WAP-enabled GSM mobile phone or a WAP-enabled portable computer. With this device a program, for example a WAP browser, can be executed and can connect as a client to a WEB or WAP server 5 and therefore can access data on this server.

The WEB or WAP server 5 contains WML and/or HTML-pages that are offered for example by a service provider (for example a financial institute and/or a provider in the field of e-commerce). Often the service providers as well as the end users wish that the session built when a user accesses several pages is secured. Especially, it is often necessary for some data transmitted bi-directionally between terminal 1 and server 5 to be

end-to-end secured and for no third party, not even the operator of the mobile phone network, to be able to decrypt that data. Furthermore, a mutual authenticating of the service provider and of the mobile subscriber is necessary.

The user of the terminal can access a secured page, for example for a transaction, by clicking on the corresponding URL of a secured or non-secured page. The URL of the page defined by the service provider reads for example http://www.sp1.com:50443, where http://www.sp1.com is the URL-address of the service provider and 50443 his port number. In the WAP, on the other hand, the sequential port number fields 920x are used.

According to the invention, the URL in the WML and/or HTML pages of the service provider is written in such a way as to determine the desired kind of session (end-to-end secured, standard secured, non-secured), from this URL, among others from the URL address and/or the port number.

Reference number 3 also shows a gateway connected to the mobile phone network 2. The gateway receives the packets from subscriber 1 and decrypts the first packet or packets in each session until an application 314 can extract the port number and the URL of the requested WEB and/or WAP pages from the packets.

As soon as these indications have been found, the application 314, based on the information given by the administrator of the gateway, decides how the packets should be handled. Specifically, the application determines whether the session between the terminal 1 and the server 5 should be end-to-end secured. This is the case, for example, if the port number (for example 50443) is in a list built by the administrator of the gateway.

Gateway 3 uses an additional protocol layer 310 (tunnel layer) that is controlled by the application 314 (arrow 315). If the session is to be secured, the tunnel layer 310 is controlled so that all following packets of

the session are transparently led through the gateway and routed to the target address of server 5, without being converted and, more importantly, without being decrypted.

The session's packets, still secured with WTLS, are then routed over network 4 and received by server 5 in the secured domain of the service provider. The network 4 can for example consist of the internet or of a rented telephone line. The server 5 comprises a proxy 52, to be explained later, a conventional gateway 50, and a database 51, where WEB and/or WAP contents are stored.

The proxy 52 in server 5 of the service provider is constructed in such a way that it can receive WTLS secured sessions. It comprises preferably a complete WAP protocol stack and can be realized by an expert by easily adapting standard software. In this proxy, received WTLS-secured WDP datagrams are examined with the certificate of a trusted third party, decrypted and converted to normal TCP-IP datagrams, where the http session is optionally SSL-secured. The converted TCP-IP packets are routed to the WAP or WEB server 50, which may possibly implement another protocol conversion, so that the received request can be processed by database system 51.

Alternatively, the datagrams can be decrypted and encrypted with a session key, the keys of which are generated with the help of a certified, public key during the key agreeing phase.

The answer from WEB or WAP server 50, for example the requested WEB and/or WAP page, is sent by server 50 in the other direction, converted and secured with WTLS services in proxy 52 and routed through the "tunnel layer" 310 in gateway 31 to the terminal 1 of the subscriber, where the complete connection between server 5 and terminal end user 1 is secured with WTLS.

Datagrams that do not need end-to-end secured data transmission because of the contained URL and/or the port number, are decrypted

in gateway 31 according to the conventional solution as recommended by the WAP forum through all layers of protocol by the gateway 2, re-secured with TLS/SSL and routed to the URL address indicated in the packets. For example, sessions with port number 80 are handled and sent on like normal HTTP sessions.

Answers from server 5 (for example the requested WEB and/or WAP pages) not needing any WTLS securing between server and gateway 3 are dealt with by the proxy application 524 through a tunnel layer in the proxy (arrow 315) and only secured with WTLS services in the gateway 3.

This embodiment does not require any change of the browser in terminal 11 and demands only a relatively simple proxy 53, capable of receiving WTLS sessions, with the service provider 5. However, the software implementation in the gateway can prove to be difficult.

The second embodiment, shown in figure 4, allows this problem to be avoided by an easily implementable modification of the application (for example the browser) in terminal 1. In this embodiment, the URL address and the port number of the requested WEB and/or WAP page are copied by the browser 10 into each packet (WDP datagram) of the session. These packets are then sent over mobile phone network 2 to gateway 3 where the port number and the URL are analyzed to determine the further handling of the packets.

The advantage of this embodiment consists in the fact that the analyses and further handling of the packets can be carried out in the lower layers of the protocol, amongst other in the WDP and/or WTLS layers, and that therefore only minimal modifications of the gateway 3 are necessary.

A table 321 in gateway 3 or in a router (not shown) in front of the gateway indicates how the packets are to be handled according to port number and URL, and especially which packets are to go transparently through the tunnel layer 320. This table can preferably be configured and

adapted by the administrator of gateway 3 without having to restart the gateway in order to be able to update the configuration during its operation. Data in the table can preferably only be changed by the administrator or people with administrator authority.

The table in gateway 3 could contain the following lines:

	Entered URL address		New address (issued by Gateway)		Remarks
	Address	Port number	Address	Port number	
1	138.10.20.30	8040	140.50.60.70	12345	Packets with this address are sent transparently to the new address. The port number is replaced (Mapping).
2	*.*.*.*	50443	*.*.*.*	50443	Star wildcard allows to set the same conditions for all servers with the same port number.
3	138.10.20.40	*	138.10.20.40	*	Same as above, but without DNS lookup
4	www.sp1.com	*	www.sp1.com	*	All URLs of the sp1 have to go through the tunnel layer
5	www.sp1.com	80	www.sp1.com	80	All connections with port number 80 through tunnel layer
6	www.sp1.ch	50443	www.sp1.ch	50443	sp1 demands that all sessions with port number 50443 be sent through the tunnel layer
7	www.sp2.ch	443	www.sp2.ch	443	sp2 demands that all sessions with port number

					443 be sent through the tunnel layer. Therefore, no SSL is used with port 443. SSL can then be used by the proxy for example.
8	...				

The administrator of the gateway 3 will preferably offer a range of URL addresses and/or port numbers to the service provider. Service provider SP1, SP2 etc. can then reserve for themselves one or several URL, or port numbers or combinations of both, and advise the administrator 3 to send on transparently packets with this URL and/or port number.

The figure 5 shows as an example how the packets sent by different end users 1_1 to 1_4 are handled by gateway 3 according to their URL address and/or port number.

The described system in this example consists of three servers 5_1, 5_2 and 5_3 of three different service providers sp1, sp2 and sp3. The following four pages are stored in the first server 5_1 (5_2 resp.):

- a non-secured WEB page with the address www.sp1.com:80 (www.sp2.com:80 resp.)
- a WEB page with the address www.sp1.com: 443 (www.sp2.com: 443 resp.), SSL secured only (no end-to-end security)
- a WEB page with the address www.sp1.com: 50443 (www.sp2.com: 50443 resp.), WTLS secured (end-to-end security)

- a WAP page with the address www.sp1.com: 50443 (www.sp2.com: 50443 resp.), WTLS secured (end-to-end security)

In server 5_3 of the third service provider sp3 only two pages are stored:

- a non-secured WEB page with the address www.sp3.com:80

- a WEB page with the address www.sp1.com: 443, SSL secured only (no end-to-end security)

The first user 1_1 wants to access the secured pages www.sp1.com:443 and www.sp1.com:50443 of the service provider sp1 in server 5_1, by sending a GET(URL) request with corresponding URLs to gateway 3. The gateway 3 recognizes, on the basis of the table 321 and the URL and/or port number contained in the datagram, what security is required by these pages. In the first case (SSL security), all datagrams of the session are decrypted in gateway 3 and a conversion from WTLS to SSL is executed. In the second case (end-to-end security with WTLS), all datagrams of the session are sent on transparently to server 5_1 without being decrypted.

The second user 1_2 wants to access the secured pages www.com:50443 sp1. and www.sp1.com:50443 of the service provider sp2 in server 5_2 demanding end-to-end security. Datagrams with this address are recognized in gateway 3 and sent on transparently through the tunnel layer to the server 5_2.

The third user 1_3 wants to access the page www.sp3.com:443 of the service provider sp2 in server 5_2 , demanding a security ensured by TLS/SSL. WTLS secured datagrams with this address are recognized in gateway 3, converted through all layers of the protocol stack, secured with TLS/SSL and sent on to the server 5_3.

The fourth user 1_4 wants to access the non-secured page www.sp3.com:80 of the service provider sp2 in server 5_2. WTLS secured packets with this address are recognized in gateway 3, converted through all layers of the protocol stack sent on to the server 5_3, without securing them over the network 4.

This embodiment demands only minimal adaptations of the gateway 3. However, the browser applications in the terminals 1 have to be slightly adapted, which can prove to be difficult for many providers.

We will now describe a third embodiment of the invention avoiding this disadvantage.

In this embodiment, sessions needing end-to-end security are recognized according to the URL address and/or the port number as in the first and second embodiment. Instead of sending on the sessions transparently through the tunnel layer, the gateway in this case sends to the terminal 1 a standardized redirect command with the address and port number of the service provider indicated in the table and other parameters for the identification of gateway 5, such as a dial-in number.

The transmission address (address, port number, dial-in number etc.) in the redirect command is preferably extracted from a document available from a WEB or WAP server 5. The redirect command can also contain this or another document or the address of such a document in which the transmission address is contained. In the document, different address areas can preferably be indicated with a string pattern, for example with an * asterix.

The application in terminal 1 receiving this redirect command reacts by sending now the packets previously sent to the gateway 3 again directly to the indicated address of the service provider indicated in the redirect command.

All packets in the session are directly transmitted between the terminal 1 and the server 5 until the end user sends another URL that cannot be proceeded by the server 5 (for example if the requested page is not located on this server). In this case, the session is interrupted by the server 5 and the following packets are re-sent again to the gateway 3.

If no end-to-end security is necessary, no redirect command is sent by the gateway 3. In this case, all packets during the secured session are sent through the gateway 3.